Verbale di accordo
in tema di "Cyber Security"

Milano, 13 aprile 2018

Tra UniCredit,

e la Delegazione sindacale del Gruppo di UniCredit,

FABI:
FIRST/CISL:
FISAC/CGIL:
UILCA/UIL:
UNITA' SINDACALE:

Premesso che

UniCredit ha dichiarato che, a fronte della forte e continua evoluzione delle modalità di attacco tramite sistemi informatici compiuti con metodologie non convenzionali, in un ottica di abbattimento del rischio informatico a cui UniCredit è esposta, si rende improcrastinabile adottare nuove soluzioni informatiche finalizzate all'individuazione di anomalie di sicurezza non riconoscibili dai sistemi tradizionali oggi utilizzati;

le predette soluzioni sono quindi finalizzate a minimizzare i rischi di sicurezza del patrimonio aziendale, rafforzando la capacità di intercettare possibili minacce provenienti sia da utenti interni sia da fonti esterne;

il presidio di sicurezza aziendale in materia di "cyber security" sarà implementato integrando gli attuali sistemi con una innovativa soluzione informatica "comportamentale" descritta diffusamente alle Organizzazioni Sindacali nel corso di appositi incontri (e sinteticamente nell'allegato tecnico) e adeguando conseguentemente i processi interni di controllo;

considerato che

l'art. 4 della legge 300/70 recita che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo con le associazioni sindacali comparativamente più rappresentative sul piano nazionale;
L'Azienda ha dichiarato che l'introduzione della nuova soluzione di "User & Entities Behavioral Analytics" (monitoraggio comportamentale di utenti e asset), è indispensabile per comprendere, rilevare, prevenire comportamenti anormali e/o sconosciuti da parte di: utenti interni (dipendenti), di soggetti esterni (terze parti con cui UniCredit collabora) o di attaccanti esterni (hackers), che si possono

concretizzare in incidenti informatici a vario livello (compromissione di asset, furto di informazioni aziendali e/o personali, compromissione di informazioni aziendali e/o personali, frodi), che le soluzioni di sicurezza tradizionali non sono in grado di rilevare o prevenire.

L'Azienda ha dichiarato che l'adozione delle misure oggetto della presente intesa è motivata esclusivamente dalla necessità di perseguire un sempre più elevato presidio di sicurezza del complessivo patrimonio aziendale attraverso metodologie di apprendimento automatico in grado di minimizzare i rischi e le frodi derivanti dall'utilizzo di tecnologie informatiche, in aderenza anche alle indicazioni delle Autorità europee in tema di cyber security.

tutto ciò premesso
le Parti

in relazione alle previsioni dell'art. 4 della legge 300/70 convengono quanto segue

Art.1

Le premesse formano parte integrante del presente accordo.

Art. 2

L'Azienda ha dichiarato che la soluzione di "User & Entity behavioral analytics" adottata consentirà il monitoraggio, con modalità automatiche, dell'intero traffico dati interno ed esterno alla azienda e sarà finalizzato a evidenziare comportamenti e modalità di utilizzo di tutti i dispositivi connessi alla rete aziendale non conformi a quelli previsti statisticamente dal nuovo sistema.

I dati, salvo quanto previsto dai successivi articoli, saranno trattati solo per le finalità di sicurezza di cui nelle premesse e per il periodo strettamente necessario a tali scopi, escludendo qualsiasi attività di monitoraggio del lavoratore.

Gli eventuali alert restituiti dal sistema verranno sottoposti ad una prima analisi tecnica da parte delle competenti funzioni di Security che determineranno l'effettiva presenza di anomalie rispetto ai modelli statisticamente previsti. Se l'anomalia si rivela essere un incidente di sicurezza, verrà avviato il classico processo di Security Incident Management (come per tutte le altre tipologie di incidenti di sicurezza), interamente gestito da dipendenti del Gruppo UniCredit.

I risultati di tali analisi consentiranno alle funzioni di Security la gestione delle problematiche rilevate e determineranno tutte le azioni necessarie per l'implementazione delle misure di sicurezza correttive e di contrasto.

I dati, compresi i log relativi alle anomalie riscontrate saranno conservati in stretta osservanza del norme previste dal Codice della Privacy e dalla normativa di riferimento tempo per tempo vigente.

Art. 3

Data la particolarità e complessità della materia, qualora si rendesse opportuna la visualizzazione di una singola utenza, ~~data la particolarità e complessità della materia,~~ questa potrà avvenire esclusivamente da parte di personale dipendente appartenente alle predette funzioni di Security, di Audit oltre che dalle Forze dell'Ordine; la visualizzazione della singola utenza potrà avvenire esclusivamente per le finalità sopra descritte di sicurezza del complessivo patrimonio aziendale e della tutela della clientela, restando pertanto escluso ogni utilizzo delle informazioni ottenibili ai fini della valutazione delle prestazioni sia sotto il profilo quantitativo sia qualitativo, né a fini disciplinari fatti salvi i casi di dolo e colpa grave.

Art. 4

Qualora, a seguito delle attività di cui al precedente articolo ~~4~~ 3, emergessero elementi di attenzione riconducibili alla attività di un dipendente che possano avere anche rilevanza ai fini disciplinari, le competenti funzioni delle Risorse Umane forniranno le necessarie comunicazioni al dipendente interessato.
Quest'ultimo potrà richiedere la visione degli elementi rilevati e farsi assistere da un rappresentante aziendale di una delle Organizzazioni Sindacali firmatarie del presente accordo cui conferirà apposito incarico in forma scritta.
Quanto previsto ai commi che precedono avverrà in forma preventiva rispetto alle procedure previste dall'art. 7 della legge 300/70.

Art. 5

L'azienda fornirà agli OdC delle rispettive Aziende apposita informativa sull'andamento dell'utilizzo del nuovo sistema di difesa informatica di cui al presente accordo, con le modalità che verranno individuate tra le Parti aziendali in ogni azienda.
Le Parti firmatarie del presente accordo si impegnano a favorire la sottoscrizione del presente verbale agli OdC di tutte le Aziende interessate nel più breve tempo possibile.
L'efficacia di quanto previsto nei precedenti articoli decorre dalla data di sottoscrizione del presente verbale di accordo.

UNICREDIT

FABI FIRST/CISL FISAC/CGIL UILCA/UIL UNISIN

Allegato tecnico
(descrizione della soluzione informatica finalizzata
all'individuazione di anomalie di sicurezza)

Soluzione informatica finalizzata all'individuazione di anomalie di sicurezza.

Gli strumenti di sicurezza comportamentale aiutano a comprendere, partendo da una grande quantità di dati provenienti da diverse fonti di informazione e utilizzando una combinazione di metodi analitici avanzati, se l'attività degli utenti e di altre entità aziendali denominati "assets" (host, applicazioni, traffico di rete e archivi di dati) stanno violando regole aziendali (es: abuso di sistemi informatici o di informazioni digitali). In tal caso l'evento verrebbe contrassegnato come deviazione rispetto ai profili di comportamento standard definiti dall'azienda, presentando un'analisi dell'anomalia di sicurezza informatica verificatasi nell'interazione tra utente e asset.
L'analisi dell'anomalia può dar seguito a due eventi:

- Se confermata, si procede con l'apertura di un incidente informatico a sistema, avviando il processo di Security Incident Management
- Altrimenti, trattasi di falso positivo per cui l'analisi si ferma e l'utente può continuare con la normale operatività, il sistema viene istruito di NON notificare più la tipologia di evento che è risultata falso positivo

Lo strumento di analisi comportamentale è fornito dall'azienda Securonix, la cui adozione porterà i seguenti miglioramenti in ottica di abbattimento del rischio informatico a cui UniCredit è esposta:
• rafforzamento del livello di sicurezza interno (es: prevenire esfiltrazione di dati personali e aziendali da parte di utenti compromessi che utilizzano metodologie non convenzionali, quindi non riconoscibili dagli attuali sistemi di sicurezza messi in campo);
• rafforzamento del livello di sicurezza esterno per casi d'uso orientati alla rilevazione di minacce (es: hacker che, tramite l'utilizzo di software malevolo avanzato non riconoscibile dagli attuali sistemi di sicurezza in campo, violano le difese perimetrali rubando le credenziali interne dei dipendenti e compromettono asset informatici utilizzandoli per perpetrare azioni illegali nei confronti di UniCredit);

Il sistema è mirato a identificare, testare e, sussistendo le condizioni, implementare una soluzione di User Behavioral Analytics per comprendere meglio, rilevare, prevenire comportamenti anormali / sconosciuti di utenti (dipendenti) che si materializzano in incidenti informatici a vario livello (compromissione di asset, furto di informazioni aziendali e/o personali, compromissione di informazioni aziendali e/o personali) e che le soluzioni di sicurezza tradizionali non sono in grado di rilevare / prevenire.
L'analisi degli eventi derivanti da un alert di sicurezza comportamentale fa affidamento sul concetto "Anomaly Detection" (individuazione anomalie) ovvero la capacità di analizzare rapidamente enormi volumi di dati e di identificare (sfruttando tecnologie di apprendimento automatico) modelli non conformi a quelli previsti statisticamente, che daranno luogo ad un incidente di sicurezza.
I dati utilizzati dal sistema di analisi sono di proprietà di UniCredit e gestiti e custoditi in strutture del Gruppo UniCredit.
Allo scopo è stata scelta l'azienda SECURONIX.